REMARKS

Claims 1, 2, and 4-20 are currently pending. The Examiner has rejected Claims 12 and 17 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Additionally, the Examiner has rejected claims 12, 14, and 16 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,779 to England et al ("England"). The Examiner has also rejected claims 1, 2, 4-11, 13, 15, and 17-20 under 35 U.S.C. § 103(a) as being unpatentable over England in view of U.S. Patent No. 5,708,709 to Rose ("Rose"). Independent Claim 1 has been currently amended. The following remarks are considered by Applicants to overcome each of the Examiner's outstanding rejections. An early Notice of Allowance is therefore requested.

I. Summary of Relevant Law

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. The determination of obviousness rests on whether the claimed invention as a whole would have been obvious to a person of ordinary skill in the art at the time the invention was made. In determining obviousness, four factors should be weighed: (1) the scope and content of the prior art, (2) the differences between the art and the claims at issue, (3) the level of ordinary skill in the art, and (4) whatever objective evidence may be present. Obviousness may not be established using hindsight or in view of the teachings or suggestions of the inventor. The Examiner carries the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness and must show that the references relied on teach or suggest all of the limitations of the claims.

II. REJECTION OF CLAIMS 12 AND 17 UNDER 35 U.S.C. § 112, FIRST PARAGRAPH

Examiner contends that claims 12 and 17 added material that is not supported by the original disclosure, namely that the operating system is approved to be loaded on that specific computer platform alone. Office Action (1/31/06), P. 6. Amended Claim 1 and claims 12 and 17 all require "...that said operating system is approved to be loaded on that specific computer platform alone." Contrary to the Examiner's contention, this is taught by the original specification.

The specification describes at least two methods of ensuring security: (1) use of public/private signatures (figs. 2-3) and (2) the use of encryption/decryption keys (figs. 4-7). No where in the specification is the use of either public/private signatures or encryption/decryption keys limited to specific programs or electronic data. Rather, one example of the use of each of these security measures is supplied.

An example of using public/private signatures is given in the context of operating system ("O/S") security. Nothing in this example limits the use of public/private signatures to O/Ss alone. In fact, the specification explicitly makes it clear that O/S verification is not limited to this method. See, Application, P. 6, Lns. 20-22. An example of using encryption/decryption keys is given in the context of application programs and object files security. As with the example of public/private signatures, nothing in this example limits the use of encryption/decryption keys to application programs and object files alone. One of ordinary skill in the art would be able to decide which of these two methods was required to achieve a desired result, and then use the disclosure of the specification to implement the appropriate method. In addition, the specification clearly states:

> "The present invention is not to be considered limited in scope by the preferred embodiments described in the specification. Additional advantages and modifications, which readily occur to those skilled in the art from consideration and specification and practice of this invention are intended to be within the scope and spirit of the following claims:"

Application, P. 18, Lns. 1-6. The specification also states that one aspect of providing a secure O/S is "ensuring that the operating system is approved for the platform." Application, P. 3, Lns. 21-23. Therefore, the disclosure of the specification encompasses that encryption/decryption keys may be used in the context of O/S security.

The applicability of encryption/decryption keys to O/S verification is also demonstrated when Applicants describe an alternative embodiment involving sending public signatures to the manufacturers. See page 12, lines 16- page 13, line 2. In this alternative embodiment, the specification is still using application programs and object files as the illustrative example. However, after the explanation of this alternative, the specification states that this alternative embodiment is not available to O/S verification. See page 13, lines 3-6. If the applicant did not intend that public/private signatures and encryption/decryption keys are equally applicable to O/S, program applications, and object files, then it would have been unnecessary to have such a disclaimer. For the Examiner to read the teaching of the specification differently is unfairly narrowing and contrary to the language in the specification.

When describing the use of encryption/decryption keys, the specification states that "[s]imilar to the public/private signature keys, the public encryption key is distinctively related to a private decryption key," and that "both encryption/decryption keys are **unique to a particular computer platform** rather than a particular programmer." Application, P. 9, Lns. 8-11. As such, the specification discloses that when encryption/decryption keys are used, the electronic data associated with these keys is "unique to a particular computer platform." Conversely, this means that the specification has disclosed that, to make electronic data "unique to a specific computer platform," one can use encryption/decryption keys.

This language creates the direct support for the claim language that the Examiner contends is not supported. One of ordinary skill in the art would understand, from the above disclosure of the specification, that one could ensure an O/S is approved to be loaded on a specific computer platform alone by using encryption/decryption keys, because using such keys would ensure the O/S was "unique to a specific computer platform."

While the use of encryption/decryption keys is explained in the context of application programs and object files, nothing in the example limits encryption/decryption keys to these types of electronic data. As such, encryption/decryption keys can be used in the context of an O/S. This is especially so since the specification illustrates that O/Ss are an example of electronic data the may require security protection. The application makes it clear that both methods, public/private signatures and encryption/decryption keys, are equally applicable to whatever electronic data is desired to be protected (e.g., O/S, application programs, object files, etc.). See, Application, P. 6, lines 20-22 and P. 8, Lns. 16-20. Since O/S, application programs, and object files are all software code, the applicability of these two methods to these objects would be understood by one of skill in the art.

All of the above portions of the specification of the Application support the claim limitation "...that said operating system is approved to be loaded on that specific computer platform alone." It is therefore respectfully requested that Examiner remove the rejection of claim 12 and 17 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

III. REJECTION OF CLAIMS 12, 14, AND 16 UNDER 35 U.S.C. § 102(E) BASED ON ENGLAND

With respect to this rejection, the Examiner contends that:

> "England discloses a computer system for content protection wherein the operating system is authenticated during the boot process before it

> is loaded (Col. 2, lines 16-40), which meets the limitations of a receiving platforms, each of said receiving platforms having firmware and an operating system, said firmware authenticating said operating system. **The fact that the operating system is authenticated on the computer system meets the limitation of the operating system being approved to be loaded on that specific computer platform alone.**"

Office Action (1/31/06), P. 7 (emphasis added). However, this misconstrues the teachings of England. Specifically, as is described in detail below, England never teaches an operating system "approved to be loaded on that specific computer platform alone." 7/18/05 Response to 3/16/05 Office Action, P. 4, Claim 12. As such Applicants respectfully assert that the Examiner's rejection stands in error.

Claim 12

Claim 12 of the current application requires:

> "a plurality of receiving platforms, each of said receiving platforms having firmware and an operating system, said firmware authenticating said operating system, **to ensure that said operating system is approved to be loaded on that specific computer platform alone**;"

7/18/05 Response to 3/16/05 Office Action, P. 4 (emphasis added).

England, however, discloses that the authentication of the operating system is "to authenticate to remote distributors that the computer is running a copy of an operating system that is trusted to provide adequate protection for digital content, and that even a legitimate user in physical possession of the computer cannot vitiate this protection." England, Col. 2, Lns. 18-23. Such an authentication relates to the features of an operating system and whether or not it has the requisite protection capabilities. Such an authentication bears no relation to the correlation of a specific operating system to a specific computer platform.

Examiner asserts that, because the authorization step of England occurs when the operating system is already installed within a computer platform, England discloses that the only computer platform that the operating system can be loaded on would be the very one

that it is installed on. Office Action (1/31/06), P. 2-3. This, however, is not necessarily the case. Should someone install the operating system via a CD-ROM, nothing in the verification of the operating system in England incorporates verifying that someone has not used that same CD-ROM to install that same operating system on another computer platform. As such, under England, it is possible to load the same operating system on multiple computer platforms.

For the above reasons, England fails to disclose the Claim 12 limitation that the operating system is approved to be loaded on a specific computer platform alone.

Claim 12 also requires:

> "said sending station including: (a) a plurality of application programs, (b) a plurality of object files, **(c) a plurality of handler programs, each associated with a separate one of said object files, and (d) a plurality of secret key encoded signatures, each distinctive to a subset of said application programs and said object files,"**

7/18/05 Response to 3/16/05 Office Action, P. 4 (emphasis added).

England fails to disclose "a plurality of handler programs, each associated with a separate one of said object files." England does disclose a single security manager 420, however, this security manager is general to all object files and is certainly not a "plurality ... associated with a separate one of said object files." England, Col. 7, Ln. 57 – Col. 14, Ln. 9.

Examiner contends that England satisfies this limitation by disclosing that the content distributor digitally signs each particular application so that it can be authenticated. Office Action (1-31-06), P. 3. This, however still discloses a single content distributor, which cannot be a plurality.

Furthermore, the above limitation states that each of the plurality of handler programs is "associated with a separate one of said object files." This claim limitation requires 2 or more handler programs, each of which is associated with one and only one object file, where none of said 2 or more handler programs is associated with the same object

file. England certainly never discloses this limitation, and Examiner never contends otherwise.

For all the above reasons, England fails to set forth this claim limitation.

Finally, Claim 12 requires:

> "each of said **handler programs being programmable to permit multi-parameter control** over access to the associated one of said object files."

7/18/05 Response to 3/16/05 Office Action, P. 4 (emphasis added).

As discussed above, England fails to disclose handler programs. England certainly fails to teach that handler programs are programmable to permit multi-parameter control over access to the associated one of said object files."

Examiner contends that England shows that modules can be assigned for handling the content of Dynamic Link Libraries ("DLLs"), which by their very nature are programmed to control access over code. Office Action (1/31/06), P. 3-4. However, the DLLs of England are only disclosed as supplying "functions to one or more programs." England Col. 5, Lns. 27-29.

The specification of the current application specifies that "(t)he object handler can use a number of parameters (publisher, expiration date, platform identifications, etc.) as criteria for access." Application, P. 14, Lns. 20-22. Such multi-parameter control is not disclosed in England by assigning modules for handling the content of DLLs. Therefore, England fails to set forth this claim limitation.

For all of the foregoing reasons, England does not contain each and every element as set forth in Claim 12. Therefore, Applicants respectfully assert that Examiner has failed to establish a prima facie case of anticipation of independent Claim 12 and corresponding claims 14 and 16 because they are dependant from Claim 12. Therefore,

Applicants respectfully request that Examiner remove the rejection of claims 12, 14, and 16 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,779 to England et al.

IV. REJECTION OF CLAIMS 1, 2, 4-11, 13, 15, AND 17-20 UNDER 35 U.S.C. § 103(A) BASED ON ENGLAND IN VIEW OF ROSE

With respect to this rejection, the Examiner contends that:

> "The fact that the operating system is authenticated on the computer system meets the limitation of **the operating system being approved to be loaded on that specific computer platform alone.**"

Office Action (1/31/06), P. 9. However, this misconstrues the teachings of England, because England does not disclose an operating system approved to be loaded on a specific computer platform alone.

Claim 1

Claim 1 has currently been amended, and currently requires:

> "a computer platform having hardware; said hardware capable of authenticating an operating system to be loaded on said hardware, **to ensure that said operating system is approved to be loaded on that specific computer platform alone**, and preventing said operating system from being loaded onto said hardware when said operating system is not authenticated;"

(emphasis added).

As discussed above, England discloses that the authentication of the operating system is "to authenticate to remote distributors that the computer is running a copy of an operating system that is trusted to provide adequate protection for digital content, and that even a legitimate user in physical possession of the computer cannot vitiate this protection." England, Col. 2, Lns. 18-23. As discussed above in relation to Claim 12, this is completely unrelated to whether or not the operating system is approved to be loaded on a specific computer platform alone. Also, as discussed above in relation to Claim 12, the fact that the authorization step of England occurs when the operating system is already installed within a

computer platform does not mean that the only computer platform that the operating system can be loaded on would be the very one that it is installed on. Therefore, England fails to set forth this claim limitation.

As such, Applicants respectfully assert that Examiner has failed to establish a prima facie case of obviousness of independent Claim 1, and corresponding claims 2 and 4-11 because they are dependant from Claim 1. Therefore, Applicants respectfully request that Examiner remove the rejection of claims 1, 2, and 4-11 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claims 13 and 15

Claim 13 is dependant from Claim 12. As discussed above, Claim 12 is allowable. Therefore, so must be Claim 13. Claim 15 is dependant from Claim 13, and is thus also allowable.

As such, Applicants respectfully assert that Examiner has failed to establish a prima facie case of obviousness of claims 13 and 15 because they are dependant from Claim 12. Therefore, Applicants respectfully request that Examiner remove the rejection of claims 13 and 15 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Claim 17

Claim 17 is a method claim similar to Claim 12 and requires:

> "authenticating an operating system to be loaded on a computer platform ... **to ensure that said operating system is approved to be loaded on that specific computer platform alone**;"

7/18/05 Response to 3/16/05 Office Action, P. 6 (emphasis added).

While examiner objects to this claim under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No.

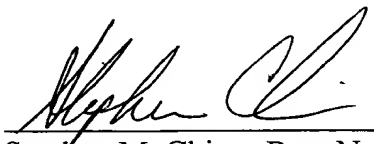
5,708,709 to Rose, Claim 17 does not contain the one limitation for which Examiner uses Rose. As such, this claim cannot be obvious over England in view of Rose.

Furthermore, as discussed in relation to Claim 12, the above Claim 17 limitation is not disclosed in England.

As such, Applicants respectfully assert that Examiner has failed to establish a prima facie case of obviousness of independent Claim 17 and corresponding claims 18-20 because they are dependant from Claim 17. Therefore, Applicants respectfully request that Examiner remove the rejection of claims 17-20 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,775,779 to England et al in view of U.S. Patent No. 5,708,709 to Rose.

Based upon the above remarks, Applicant respectfully requests reconsideration of this application and its early allowance. Should the Examiner feel that a telephone conference with Applicant's attorney would expedite the prosecution of this application, the Examiner is urged to contact him at the number indicated below.

Respectfully submitted,



SMC:JWT

Stephen M. Chin - Reg. No. 39,938
Reed Smith LLP
599 Lexington Avenue
New York, NY 10022
Tel. (212) 521-5400

500578.20076